



Reg. No.

A U H I P P O . C O M \*

**Question Paper Code : 50399****B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2017****Seventh/Eighth Semester****Computer Science and Engineering****CS 6701 – CRYPTOGRAPHY AND NETWORK SECURITY****(Common to Electronics and Communication Engineering/Information Technology)  
(Regulations 2013)****Time : Three Hours****Maximum : 100 Marks****Answer ALL questions.****PART – A****(10×2=20 Marks)**

1. Categorize Passive and Active attack.
2. State Fermat's Theorem.
3. Perform encryption for the plain text  $M = 88$  using the RSA Algorithm  $p = 17$ ,  $q = 11$  and the public component  $e = 7$ .
4. Give the significance of hierarchical key control.
5. How is the security of a MAC function expressed ?
6. Mention the significance of signature function in Digital Signature Standard (DSS) approach.
7. Write a simple authentication dialogue used in Kerberos.
8. List any 2 applications of X.509 Certificates.
9. Specify the purpose of ID Payload in Phase I and Phase II inherent in ISAKMP/IKE encoding.
10. Justify the following statement :

"With a Network Address Translation (NAT) box, the computers on your internal network do not need global IPV4 addresses in order to connect to the Internet".



## PART - B

(5×16=80 Marks)

11. a) Encrypt the following using play fair cipher using the keyword MONARCHY.  
"SWARAJ IS MY BIRTH RIGHT". Use X for blank spaces.

(OR)

- b) Discuss the properties that are to be satisfied by Groups, Rings and Fields.
12. a) Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime  $q = 83$  and a primitive root  $\alpha = 5$ .
- i) If Alice has a private key  $X_A = 6$ , what is Alice's public key  $Y_A$ ? (6)
  - ii) If Bob has a private key  $X_B = 10$ , what is Bob's public key  $Y_B$ ? (6)
  - iii) What is the shared secret key? (4)
- (OR)
- b) For each of the following elements of DES, indicate the comparable element in AES if available.
- i) XOR of subkey material with the input to the function. (4)
  - ii) f function. (4)
  - iii) Permutation p. (4)
  - iv) Swapping of halves of the block. (4)
13. a) Write down the steps involved in
- i) Elgamal Digital Signature Scheme. (8)
  - ii) Schnorr Digital Signature Scheme. (8)
- used for authenticating a person.
- (OR)
- b) With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than  $2^{128}$  bits and produces as output a 512-bit message digest.
14. a) Explain how secure electronic transaction (SET) protocol enables e-transactions in details. Explain the components involved.
- (OR)
- b) Discuss how firewalls help in the establishing a security framework for an organization.
15. a) i) Discuss the different methods involved in authentication of the source. (8)
- ii) Write about how the integrity of message is ensured without source authentication. (8)
- (OR)
- b) i) Write the steps involved in the simplified form of the SSL/TLS protocol. (8)
- ii) Write the methodology involved in computing the keys in SSL/TLS protocol. (8)